Bijlage:
Verwijdermethoden

Inleiding

Fabrikanten van systemen of componenten richten zich op het voorkomen van dataverlies als gevolg van menselijke fouten, elektrostatische lading, kosmische straling of falen van componenten. Voor het ontwikkelen van een stemprinter is juist géén permanente opslag gewenst, maar tijdelijke opslag en volledige controle over het al dan niet benaderbaar zijn van data. Technologie die zo ontworpen is dat het juist opslag of benaderbaarheid op een gecontroleerde manier beperkt, wordt slechts binnen een aantal nichemarkten gebruikt. Hierdoor is de ontwikkeling en beschikbaarheid van dergelijke technologie zeer beperkt. Een relatief bekend voorbeeld is de bankensector, die de drijvende kracht is achter de ontwikkeling van smartcards en HSM's, componenten die een veilige en gecontroleerde opslag en gebruik van cryptografische sleutels waarborgen.

Als een software of hardware component in gangbare computerarchitectuur data "verwijdert", wordt over het algemeen alleen de referentie naar die data uit een centrale index verwijderd. Dit houdt in dat de gegevens zelf er nog staan, maar het niet meer als opgeslagen geregistreerd staat en de ruimte waar de data zich bevindt beschikbaar is voor opslag van nieuwe data. Totdat data overschreven is met andere gegevens, is er feitelijk niets ondernomen om de gegevens echt te verwijderen. De reden hiervoor is dat daadwerkelijk verwijderen meestal niet nodig is, en verwijderen uit de centrale index veel sneller gaat. Ook, bijvoorbeeld, het opnieuw formatteren van een schijf levert weinig garanties. Het feit dat data in veel gevallen niet echt verwijderd is, is dan ook het basisprincipe voor veel succesvol forensisch onderzoek naar "verloren" gegevens.

In deze bijlage wordt allereerst een indicatie gegeven van de gegevens die na verwijderen achter kunnen blijven. Vervolgens wordt ingegaan op de methoden om gegevens daadwerkelijk te verwijderen.

Waar kunnen gegevens achterblijven

Zoals in de inleiding is gesteld kunnen gegevens na verwijderen op de plek waar ze stonden nog aanwezig zijn, omdat alleen de verwijzing naar de gegevens is verwijderd. Dat geldt bijvoorbeeld voor gegevens die in het interne geheugen worden verwerkt en voor gegevens die in een bestand worden opgeslagen. Daarnaast kan de standaard software en hardware die wordt gebruikt voor de verwerking van gegevens er voor zorgen dat kopieën van verwerkte gegevens of delen daarvan op andere plekken achterblijven. Dit doet zich voor bij de verwerking van gegevens door het besturingssysteem, databasemanagementsysteem, standaard programmamodules, een printer en een scherm. Voorbeelden van plekken waar verwerkte gegevens achter kunnen blijven zijn:

- Logbestanden, waarin de verwerking van gegevens wordt gelogd. Logbestanden worden gebruikt om achteraf de correcte werking van programmatuur vast te stellen of bij problemen te helpen om de oorzaak te vinden.
- Transactiebestanden, waar verwerkte gegevens tijdelijk in worden opgeslagen totdat de verwerking van de gegevens helemaal is afgerond of om het mogelijk te maken de verwerking van gegevens weer terug te kunnen draaien. Transactiebestanden worden gebruikt om de gegevensverwerking robuust te maken als zich afwijkende situaties voordoen, zoals stroomuitval of bij het optreden van fouten bij de verwerking van gegevens, dan wordt het resultaat van een lopende maar nog niet afgeronde gegevensverwerking op basis van de gegevens in het transactiebestand weer teruggedraaid.
- Geheugenoverloopbestanden (een zogenaamde page file), waarin gegevens die in het interne vluchtige geheugen staan tijdelijk worden opgeslagen als het interne geheugen daarvoor alleen

niet toereikend is. In situaties dat het beheerssysteem vastloopt kan zelfs een complete kopie van de inhoud van het vluchtige interne geheugen in een bestand terecht komen, een zogenaamde coredump.

- Cache, stukken van het interne vluchtige (niet permanente) geheugen die worden gebruikt om ingelezen gegevens of naar permanent geheugen geschreven gegevens te bewaren, om in het geval ze nog een keer nodig zijn en er dan snel over te kunnen beschikken.
- Indexbestanden, die worden aangemaakt om snel op gegevens te kunnen zoeken. In die bestanden kunnen dan delen van verwerkte gegevens terechtkomen. Een variant hierop zijn statistische gegevens die worden bijgehouden om over zoekacties te rapporteren of om zoekacties te versnellen.
- Printbestanden, waarin gegevens worden opgenomen die naar de printer worden gestuurd.
- Back-up bestanden, waarin een kopie van gegevens wordt opgeslagen om bij calamiteiten met apparatuur of fouten in de verwerking van gegevens, een eerdere stand van de gegevens weer terug te kunnen zetten.
- In gebruikte (rand)apparatuur, bijvoorbeeld in de buffer van een printer, een cache van een harde schijf, het interne geheugen van een schermcontroller of het interne geheugen dat wordt gedeeld door schermcontroller en de processor van de verwerkingseenheid.
- In een database managementsysteem, zoals een SQL database. Ook in dat geval kan bij het verwijderen van gegevens alleen de toegang tot de gegevens uit indexen wordt weggehaald, maar de gegevens zelf nog zijn te reconstrueren. Verder zal een databasemanagementsysteem voor de verwerking en toegang tot de gegevens de gegevens of delen daarvan op meerdere plekken opslaan. Dat gebeurt bijvoorbeeld voor het kunnen terugdraaien van transacties (transactielog), zoeken naar gegevens (indexen) en voor het sorteren van gegevens. Ook nadat de gegevens zelf zijn verwijderd uit de database, kunnen de daarvan afgeleiden gegevens zodoende nog elders in de database aanwezig zijn.

Complicerende factor is dat van gebruikte programmeerhulpmiddelen, standaard programmatuur, besturingssysteem en apparatuur niet of maar beperkt gedocumenteerd is waar verwerkte gegevens opgeslagen kunnen worden. Bij gebrek aan informatie daarover zal dit aan de hand van een analyse van de broncode of met testen vastgesteld moeten worden waar gegevens achter kunnen blijven. Hierbij moet dan niet alleen de reguliere gang van zaken nagelopen worden, maar ook bijzondere (fout)situaties, zoals het afbreken van de gegevensverwerking, waarbij gegevens in bijvoorbeeld een foutlog, transactielog of geheugendump achter kunnen blijven.

<u>Verwijdermethoden</u>
De beste methode om gegevens niet te hoeven verwijderen is de gegevens niet op te slaan. Tijdens de verwerking van stemkeuzen door een stemprinter zal de stemkeuze echter minimaal in het interne vluchtige geheugen opgeslagen moeten worden. Na het printen van de stemkeuze moet de stemkeuze dan uit het interne geheugen worden verwijderd. Alleen het vrijgeven van het geheugen is dan niet afdoende, want dan staat de keuze er nog in, maar zal de stemkeuze in het interne geheugen moeten worden overschreven.

Verder moet worden voorkomen dat gegevens die niet opgeslagen hoeven te worden op andere plekken terecht komen en dan toch worden opgeslagen. Dat kan bijvoorbeeld door de volgende maatregelen te treffen:

- Logging waar niet nodig uitzetten en daar waar logging wordt toegepast daarin geen gegevens op te nemen waaruit een stemkeuze is te herleiden.
- Instellingen in het besturingssysteem wijzigen zodat geen sporen van later te verwijderen gegevens ontstaan, zoals geheugenoverloop uitzetten, maken van coredumps uitzetten, cachen van gegevens uitzetten, indexering van gegevens uitzetten, direct printen in plaats van via een

printerspooler, back-ups uitzetten. Dergelijke instellingen dienen met beleid gewijzigd te worden omdat het gevolgen kan hebben ondermeer voor verwerkingssnelheid en robuustheid.
- Randapparatuur (zoals printers en beeldscherm) gebruiken die de te verwerken of verwerkte gegevens niet tijdelijk opslaat in eigen geheugen, waar direct verwerkt.

Daar waar het achterblijven van verwijderde gegevens en sporen daarvan niet is te voorkomen en deze gegevens met vrij verkrijgbare hulpmiddelen zijn te achterhalen, zullen de te verwijderen gegevens opgeruimd moeten worden. Daarvoor kunnen bijvoorbeeld de volgende maatregelen worden genomen:
- Het gebruik van een standaard programma dat verwijderde gegevens en sporen daarvan opruimt – bijvoorbeeld door ze te overschrijven – op het moment dat de gegevens worden verwijderd.
- Het gebruik van een intern commando van een database managementsysteem, opslagmedium of apparaat om verwerkte gegevens en sporen daarvan op te ruimen.
- Het verwerken van “dummy” gegevens om daarmee gegevens uit een transactielog, cache of verwerkingsgeheugen te schonen.
- Het lang genoeg tijdelijke uitschakelen van componenten zodat opgeslagen gegevens verdwijnen.

De effectiviteit van een toe te passen verwijdermethode zal uitgebreid getest moeten worden. Want er kunnen bijzondere (fout)situaties zijn waarin toch niet alle gegevens of sporen daarvan worden opgeruimd. Bij testen van de effectiviteit van een verwijdermethode zal met forensische middelen nagegaan moeten worden of er nog verwijderde gegevens zijn en zo ja waar.